

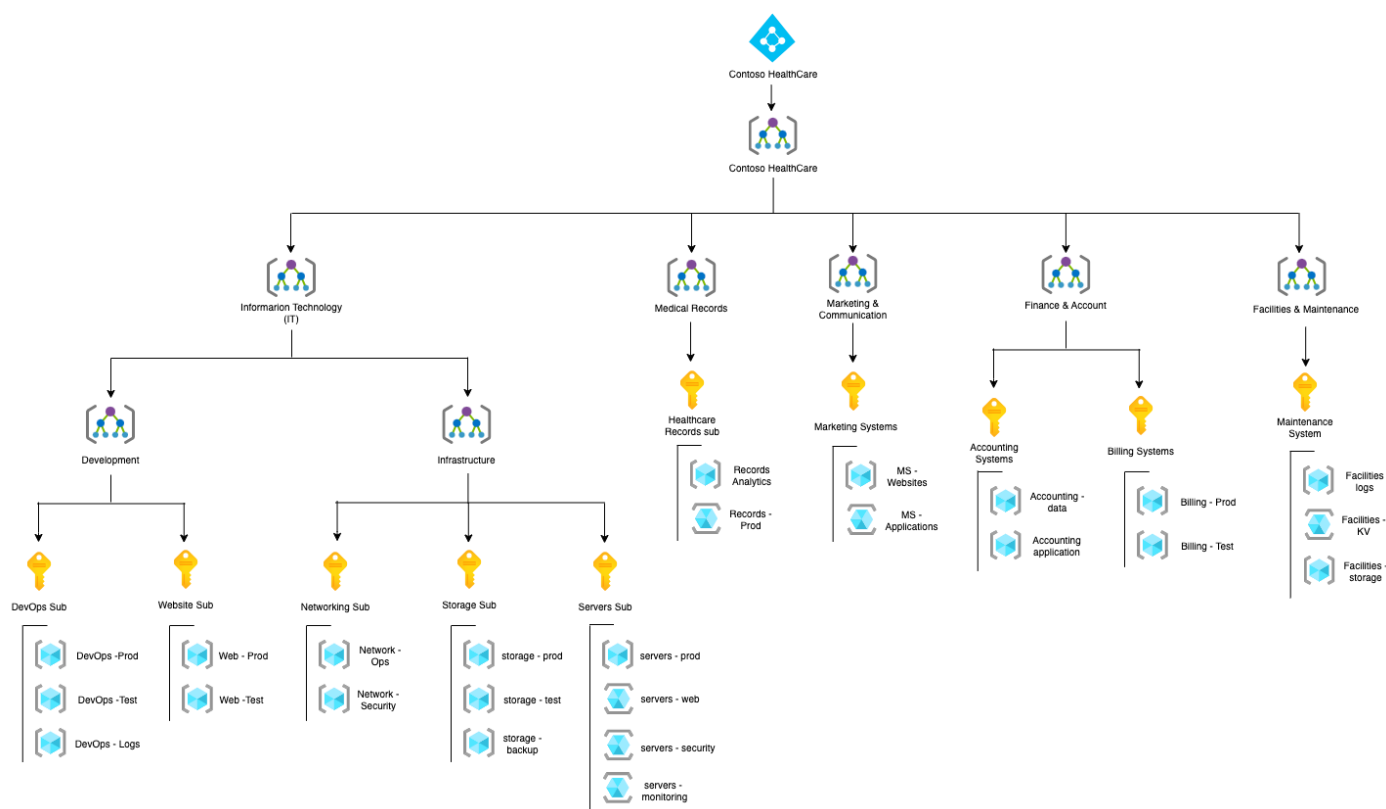
## Project: Implementing Secure Cloud Governance at “Contoso Healthcare”

In this project (scale down model), I navigated a real-world scenario assuming the role of an Azure identity engineer in a healthcare organization, “Contoso Healthcare.” The organization is in the process of transitioning into Azure cloud, and it is crucial to establish proper identity and access management along with governance controls in the Azure environment.

As the lead identity engineer on Contoso Healthcare cloud migration project, I was responsible for designing and implementing identity management, access controls, and governance processes for the new Azure environment.

- Lead the deployment and configuration of the Azure AD by integrating identities into Azure cloud.
- Implement Azure role-based access controls (RBAC) by granting least privilege based on job roles and responsibilities.
- Develop and enforce security policies on user accounts, data, and resources within the environment.
- Set up actionable budget alerts and utilization reporting.
- Implement self-service password reset for employees within the organization.

### Azure Management Group Diagram



To effectively execute this project; the implementation will be structured across four key phases:

**Part 1:** Configure the Azure AD tenant by establishing users, groups, licensing, and self-service password reset capabilities.

**Part 2:** Implement Azure role-based access controls (RBAC) by creating roles with appropriate permissions to Azure resource groups. Assign permissions to users and/or groups at the appropriate scopes to grant least privilege access.

**Part 3:** Deploying governance tools such as Azure Policy, resource locks, and tags in the environment.

**Part 4:** Optimize cost management through budgets, and alerts.

*Let's get started!*

**Part 1: Configure the Azure AD tenant by establishing users, groups, licensing, and self-service password reset capabilities.**

The focus of part one is to concentrate on deploying Azure Active Directory as the primary identity and access management provider by creating user accounts, security groups, licensing, and self-service password reset. This forms the identity foundation for assigning permissions in later phases.

**Step 1:** Select “**Create a resource**” and search for “**Azure Active Directory**.” Select “**Create**” and fill out the tenant configuration with Contoso Healthcare information. After filling out the information select “**Create**.” After these steps, we have successfully created an Azure Tenant for Contoso Healthcare Azure Active Directory.

**Create a tenant** ...

Azure Active Directory

✓ Validation passed.

\* Basics \* Configuration Review + create

Summary

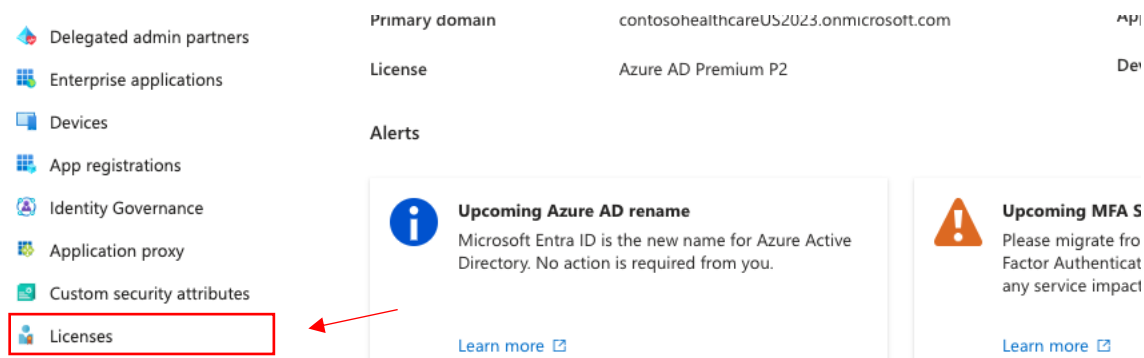
**Basics**

Tenant type	Azure Active Directory
-------------	------------------------

**Configuration**

Organization name	Contoso Healthcare
Initial domain name	contosohealthcareUS2023.onmicrosoft.com
Location	United States

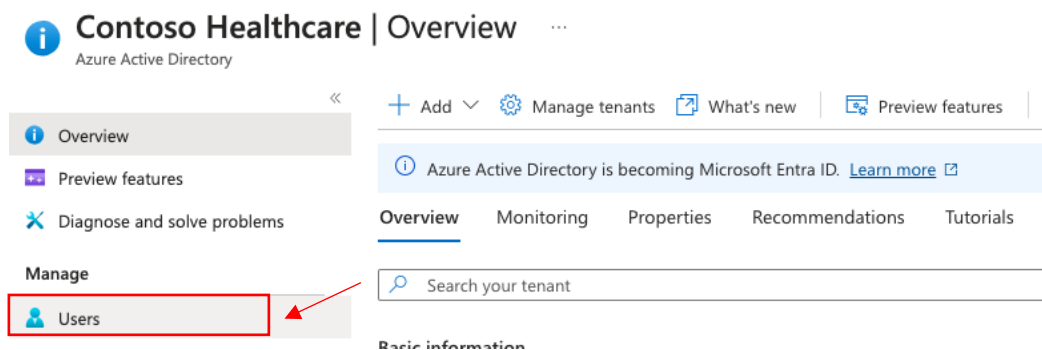
**Step 2:** Under *Contoso Healthcare Overview*, select “**Licenses**” and apply the appropriate license for this project which is Azure AD Premium P2.



After applying the correct license to Contoso Healthcare, the next step is to refresh Contoso Healthcare | Overview page to see the Azure AD Premium P2 license.

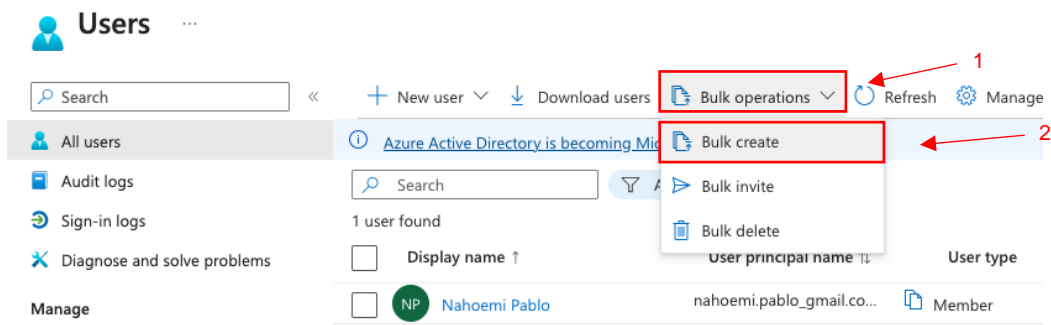
Basic information			
Name	Contoso Healthcare	Users	1
Tenant ID	479fc12f-9f6c-467f-9453-3efabe4d6daf	Groups	0
Primary domain	contosohealthcareUS2023.onmicrosoft.com	Applications	0
License	Azure AD Premium P2	Devices	0

**Step 3:** In the *Azure Portal*, locate and select “**Azure Active Directory**” from the left-hand navigation pane. Under *manage*, select “**Users**” to access user management page.



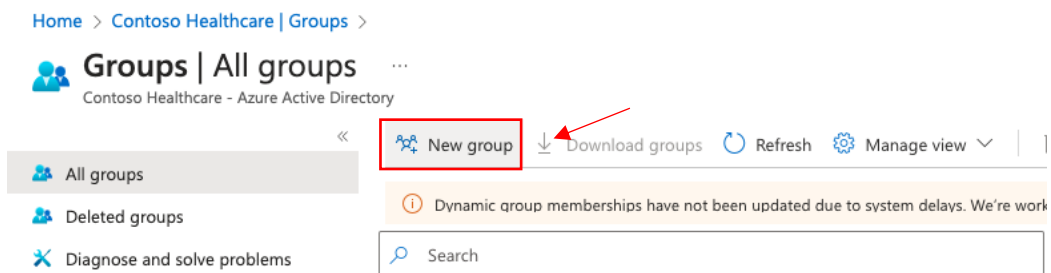
Note: For this project, I will select the “**Bulk Operations**” to create all the users simultaneously.

**Step 3:** Select “**Bulk Operations**” follow by “**Bulk Create**” and upload your csv file with the employee’s first name, last name, job title etc.



After the csv file has been uploaded successfully, you refresh the user management page to display the users in the Azure Active Directory for Contoso HealthCare.

**Step 4:** Return to the *Azure Active Directory* home page to create groups within the Azure AD. Under *manage*, select “**Groups**” follow by “**New group.**”



Fill out the “**New Group**” fields information with the department information. An example for the Information Technology department will be the following information:

**Group type:** Security

**Group name:** IT Cloud Administrator

**Group description:** Information and Technology (IT) Department is responsible for managing and maintain the organization's cloud infrastructure and services.

**Membership type:** Dynamic User

## New Group

Got feedback?

Group type \*

Security

Group name \*

IT Cloud Administrator

Group description

Information and Technology (IT) Department is responsible for managing and maintain the organization's cloud infrastructure and services.

Azure AD roles can be assigned to the group

Yes No

Membership type \*

Dynamic User

Owners

No owners selected

Dynamic user members \*

Add dynamic query

Select the **“Add dynamic query”** and fill out the dynamic membership rules for the IT Cloud Administrator Group.

Configure Rules are the following:

**Property:** department | **Operator:** Match | **Value:** Information Technology (IT)

And **Property:** usagelocation | **Operator:** Match | **Value:** US

**Dynamic membership rules** ...

Save Discard Got feedback?

Configure Rules Validate Rules (Preview)

You can use the rule builder or rule syntax text box to create or edit a dynamic membership rule. [Learn more](#)

And/Or	Property	Operator	Value
	department	Match	Information Technology (IT)
And	usageLocation	Match	US

+ Add expression + Get custom extension properties

**Rule syntax** [Edit](#)

```
(user.department -match "Information Technology (IT)") and (user.usageLocation -match "US")
```

Select **“Save”** and **“Create”** the IT Cloud Administrator group.

Home > Contoso Healthcare | Groups

**Groups | All groups** ...

Contoso Healthcare - Azure Active Directory

New group Download groups Refresh Manage view Delete Got feedback?

Dynamic group memberships have not been updated due to system delays. We're working to resolve the issue.

Search

Add filter

Search mode Contains

1 group found

Name	Object Id	Group type
IT Cloud Administrator	6bbccba2-f955-4c69-80ba-e5ca9019008c	Security

Note: I will apply the same steps to create the rest of the groups within Contoso Healthcare such as Finance and Account, Marketing and Communications Group etc

**Step 5:** Under *manage* in *Contoso Healthcare | Overview* select **“Password reset”** to configure the self-service password reset.

**Contoso Healthcare | Overview** ...

Azure Active Directory

App registrations Identity Governance Application proxy Custom security attributes Licenses Cross-tenant synchronization Azure AD Connect Custom domain names Mobility (MDM and MAM) **Password reset**

+ Add Manage tenants What's new Preview features

Azure Active Directory is becoming Microsoft Entra ID. [Learn more](#)

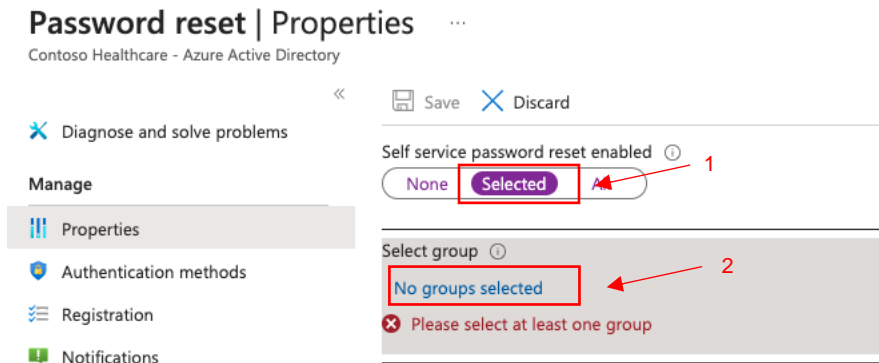
Overview Monitoring Properties Recommendations Tutorials

Search your tenant

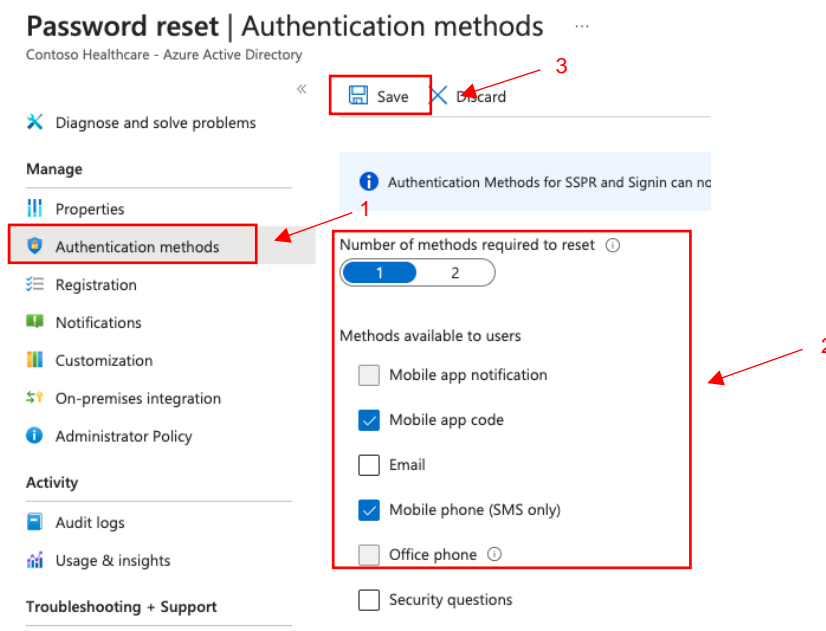
**Basic information**

Name	Contoso Healthcare
Tenant ID	479fc12f-9f6c-467f-9453-3efabe4d6daf
Primary domain	contosohealthcare152023.onmicrosoft.com

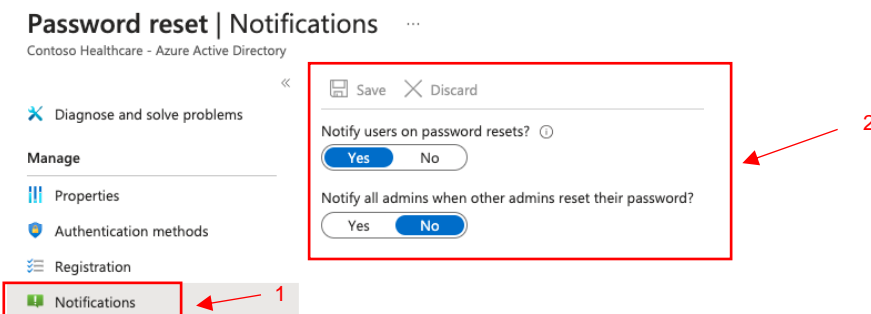
Under *self-service password reset enabled*, click on **“Selected”** and then select **“No groups selected”** to add the IT Cloud Administrator group to the password reset properties and **“Save.”**



We still need to applied authentication methods to ensure security to the self-service password reset. Select **“Authentication methods”**, follow by selecting the **“Number of methods”** and the required authentication methods and select **“Save”**.



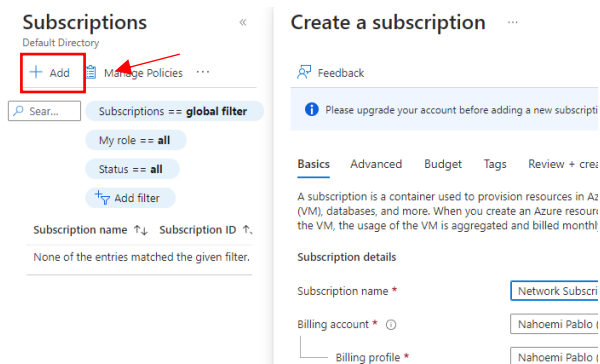
To add an additional layer of security, I would configure the password reset notification. Select **“Notifications”** and select **“Yes”** to notify users on password resets and **“No”** to notify the admin of this change.



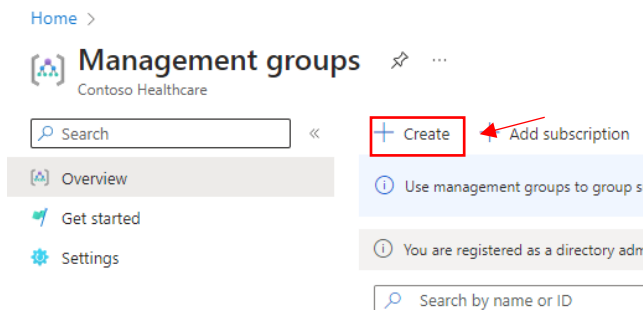
## Part 2: Implement Azure role-based access controls (RBAC) by creating roles with appropriate permissions to Azure resource groups. Assign permissions to users and/or groups at the appropriate scopes to grant least privilege access.

The objective of the second phase involves creating and assigning Azure roles with specific permissions to users and groups based on their responsibilities.

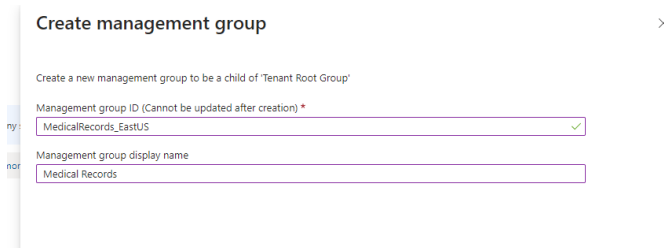
**Step 1:** To configure *subscription*, we start by searching for “**Subscriptions.**” In subscription select “**+ Add**” then fill up the subscription information and select “**Review + create**”



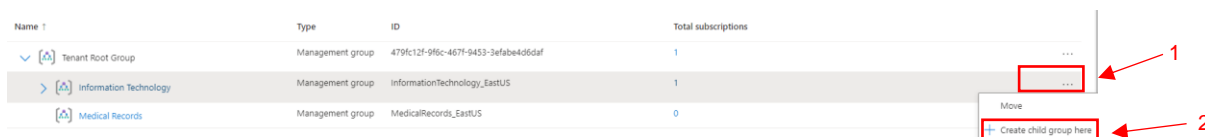
**Step 2:** To configure *Management Group* we start by searching for “**Management Group.**” In management group select “**Create**” to develop a new management group to be a child management group of the “Tenant Root Group”



Fill out the management group information according to the Azure Management Diagram. Applied the same step for each management group in the diagram.



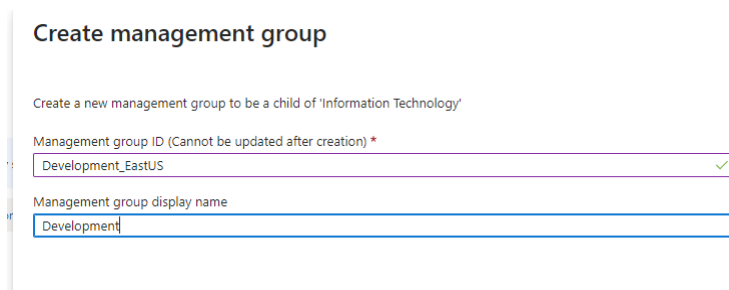
For illustration, I will continue to develop the management group for Information Technology. The Information Technology management group has two child groups: Development and Infrastructure. Select “...” and then “+ Create child group here” repeat this step to create both child groups.



The screenshot shows a table of management groups. The 'Information Technology' group is selected, and a context menu is open with the option '+ Create child group here' highlighted. Red arrows point to the '...' button and the '+ Create child group here' option.

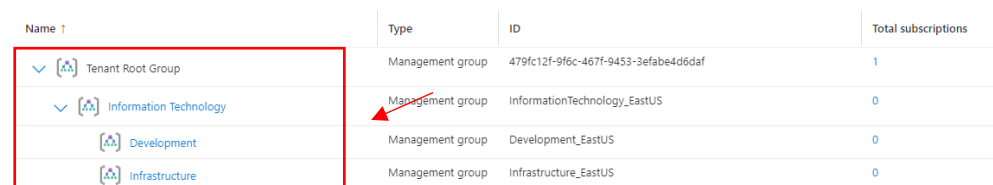
Name	Type	ID	Total subscriptions
Tenant Root Group	Management group	479fc12f-9f6c-467f-9453-3efabe4d6daf	1
Information Technology	Management group	InformationTechnology_EastUS	1
Medical Records	Management group	MedicalRecords_EastUS	0

Fill out the information for the child of “**Information Technology**” management group and “**Submit.**”



The screenshot shows the 'Create management group' form. The 'Management group ID' field is filled with 'Development\_EastUS' and the 'Management group display name' field is filled with 'Development'. A green checkmark is visible next to the ID field.

By pressing the refresh button, the new management groups will appear under their parent group(s). See below illustration.



The screenshot shows the updated list of management groups. The 'Information Technology' group now has two child groups: 'Development' and 'Infrastructure'. A red box highlights the 'Information Technology' group and its children. A red arrow points to the 'Management group' label for the 'Development' group.

Name	Type	ID	Total subscriptions
Tenant Root Group	Management group	479fc12f-9f6c-467f-9453-3efabe4d6daf	1
Information Technology	Management group	InformationTechnology_EastUS	0
Development	Management group	Development_EastUS	0
Infrastructure	Management group	Infrastructure_EastUS	0

To finalize configuring the management groups in Contoso Healthcare, we need to add the subscription to each management group within the organization. The management group “Infrastructure” has three subscriptions: Networking Sub, Storage Sub, and Servers Sub. Let’s configure the subscriptions for “Infrastructure” management group.

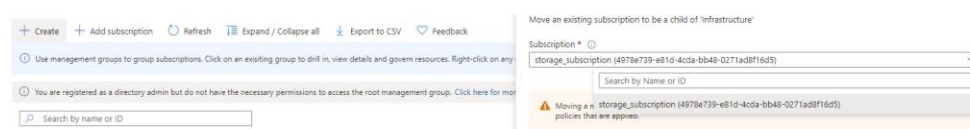
**Step 3:** At the infrastructure management group level, select “...” then “+ add subscription here.”



The screenshot shows the management groups list with the 'Infrastructure' group selected. A context menu is open with the option '+ Add subscription here' highlighted. Red arrows point to the '...' button and the '+ Add subscription here' option.

Name	Type	ID	Total subscriptions
Infrastructure	Management group	Infrastructure_EastUS	0
Medical Records	Management group	MedicalRecords_EastUS	1

In the new window, select the subscription name and select “**Save**”.



The screenshot shows the 'Add subscription' dialog box. The 'Subscription' field is filled with 'storage\_subscription (4978e739-e81d-4c0a-bb48-0271ad8f16d5)'. A warning message at the bottom states: 'Moving a n: storage\_subscription (4978e739-e81d-4c0a-bb48-0271ad8f16d5) policies that are applied.'

By pressing the refresh button, the subscription will appear under their parent group(s). See below illustration.



Showing 1 subscriptions in 4 groups

Name	Type	ID	Total subscriptions
▼ Tenant Root Group	Management group	479fc12f-9f6c-467f-9453-3efab4d6daf	1
▼ Information Technology	Management group	InformationTechnology_EastUS	1
▼ Development	Management group	Development_EastUS	0
▼ Infrastructure	Management group	Infrastructure_EastUS	1
storage_subscription	Subscription	4978e739-e81d-4cda-bb48-0271ad8f16d5	

**Step 4:** Develop *resource groups* by searching for “**Resource groups**.” In resource group select “**Create**” to develop a new resource group. Fill out the resource group page with the following information:

**Subscription:** storage\_subscription

**Resource group:** storage-prod

**Region:** (US) East US

Leave tags blank for now and follow by “**Review + create**” then “**Create**.”

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

**Project details**

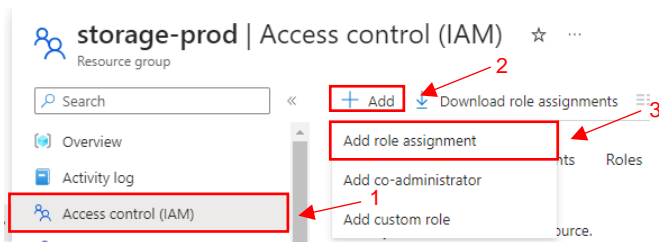
Subscription \*

Resource group \*

**Resource details**

Region \*

**Step 5:** In the resource group named “**Storage-prod**” select “**Access control (IAM)**” follow by “**+ Add**” and select “**add role assignment**.”



**Step 6:** In the *Access control (IAM)* page, select “**Privileged administrator roles**” and choose the role needed for the employee. For this project, we will select “**Contributor**.”

Role Members Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Assignment type

Job function roles

Grant privileged administrator access, such as the ability to assign roles to other users.





⚠ Can a job function role with less access be used instead?

Search by role name, description, or ID

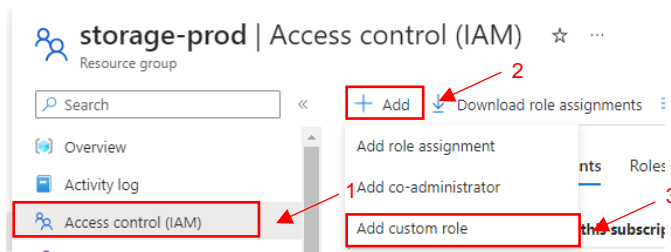
Type: All Category: All

Name	Description
Owner	Grants full access to manage all resources, including the ability to delete resources.
Contributor	Grants full access to manage all resources, but does not allow you to delete resources.

In the member tab, we select “**+ select members**”, select the member and “**Review + assign.**” For the storage-prod resource group we have an owner and a contributor.

Name	Type	Role
Contributor		
<input type="checkbox"/>  Jeff Fisher jfisher@contosohealthcareUS20...	User	Contributor 
Owner		
<input type="checkbox"/>  Linda Carter lcarter@contosohealthcareUS20...	User	Owner 

**Step 7:** To create a custom role, in resource group named “**Storage-prod**” select “**Access control (IAM)**” follow by “**+ Add**” and select “**add custom role.**”



In the “**Create a custom role**” page fill out the information.

### Create a custom role

Basics Permissions Assignable scopes JSON Review + create

To create a custom role for Azure resources, fill out some basic information. [Learn more](#)

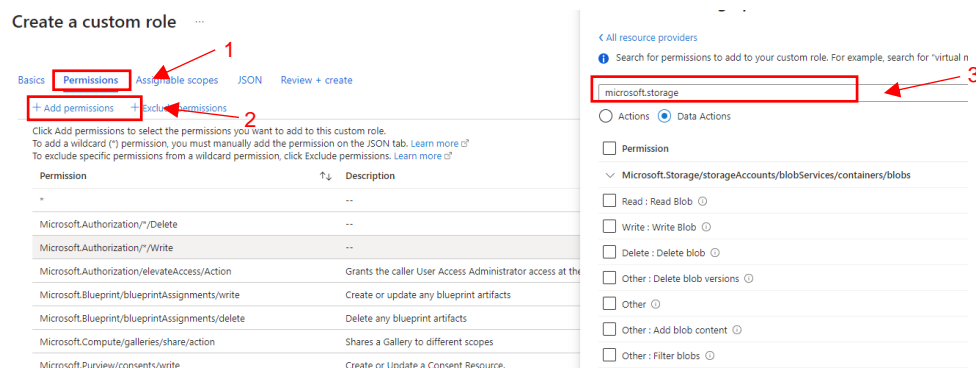
Custom role name \*

Description

Baseline permissions ☒ Clone a role ☐ Start from scratch ☐ Start from JSON

Role to clone

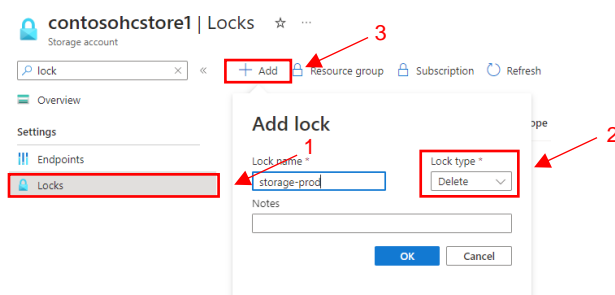
Review the *permission* tab then select “**+ Add permission.**” Search “**Microsoft.storage**” and review/select the “**Actions**” and/or “**Data Actions**” you would like to add to the role.



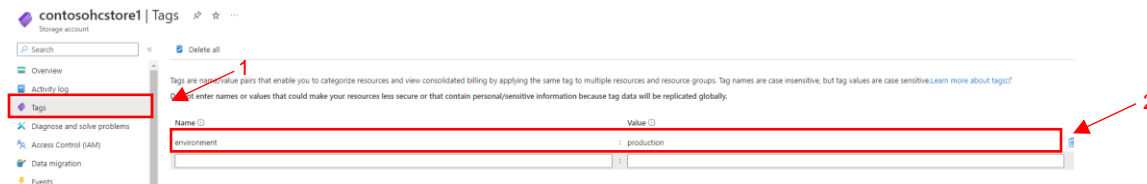
## Part 3: Deploying governance tools such as Azure Policy, resource locks, and tags in the environment.

The purpose of Part 3 is implementing governance controls in the environment through Azure Policy, resource locking, and tagging strategies. This provides organizational guardrails and resource consistency through policies, locks to restrict changes, and metadata tags.

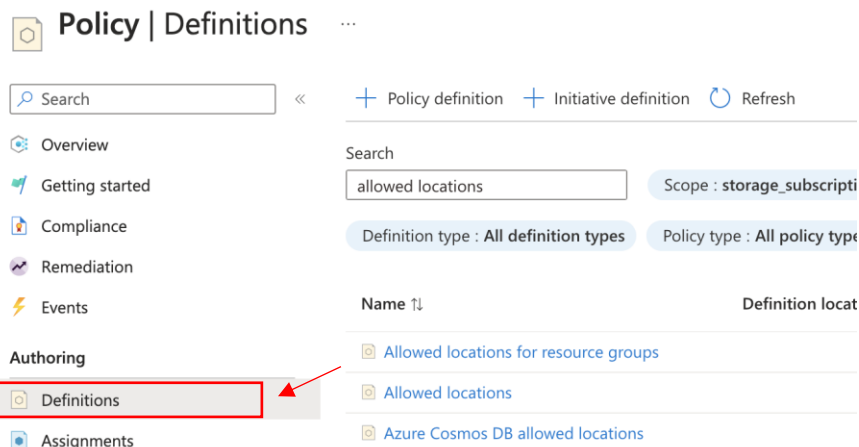
**Step 1:** In your resource, in this case “**contosoahcstore1**” which is a storage account in “**storage-prod**” resource group. Search or scroll for “**Locks**” then select “**+ Add**” and fill out the “**lock name**”. Change lock type to “**Delete**” to prevent accidental deletes.



**Step 2:** In “**contosoahcstore1**” search or scroll for “**Tags**” and fill out the tag name and value follow by apply.



**Step 3:** Search for “**Policy**.” In *Policy overview page*, select “**Definitions**” then filter the list to find “**Location**” and select “**Allowed locations**.”



Note: This policy will allow resources to be deployed in a specific location.

After locating the policy, select “**Assign.**”

Home > Policy | Definitions >

## Allowed locations

Policy definition

**Assign** Edit definition Duplicate definition Delete definition

Essentials

Name : Allowed locations

Description : This policy enables you to restrict the locations your organization can specify when deploying resources. Use to enforce your geo-c...

Available Effects : Deny

Category : General

Definition Assignments (0) Parameters

The next step in **Step 3** is to select “...” and choose the scope of the policy on the appropriate level such as Management Group, Subscription or Resource Group level and “**Select.**”

Home > Policy | Definitions > Allowed locations >

## Allowed locations

Assign policy

Basics Advanced Parameters Remediation Non-compliance messages Review + create

Scope

Scope Learn more about setting the scope \*

Exclusions

Optionally select resources to exclude from the policy assignment.

Basics

Policy definition

Scope

Management Group

Information Technology (InformationTechnology\_EastUS)

Development (Development\_EastUS)

Infrastructure (Infrastructure\_EastUS)

Subscription

storage\_subscription

Resource Group

storage-prod

Modify the *Assignment name* to “**Allowed locations-EastUS**” and leave everything else to default then click “**Next**” to the “**Parameters**” tab.

Home > Policy | Definitions > Allowed locations >

## Allowed locations

Assign policy

Basics Advanced **Parameters** Remediation Non-compliance messages Review + create

Scope

Scope Learn more about setting the scope \*

storage\_subscription/storage-prod

Exclusions

Optionally select resources to exclude from the policy assignment.

Basics

Policy definition

Allowed locations

Assignment name \*

Allowed locations-EastUS

Description

Policy enforcement

Enabled Disabled

Assigned by

Nahoemi Pablo

In the *parameters* tab select “**Allowed locations**” then choose “**East US**” and “**East US 2**” which are the locations that we are currently using for this project. Last, select “**Review + create.**”

[Home](#) > [Policy | Definitions](#) > [Allowed locations](#) >

## Allowed locations

Assign policy

Basics Advanced **Parameters** Remediation Non-compliance messages Review + create

Search by parameter name

☒ Only show parameters that need input or review

Allowed locations \* ⓘ

2 selected

☐ Select all

☒ East US

☐ East US (Stage)

☒ East US 2

## Part 4: Optimize cost management through budgets, alerts, and advisors to maximize value while minimizing expense.

The aim of part four is to optimize cloud expenditures through budgets, alerts, and utilization reporting. This enables proactive cost management through monitoring, and visibility.

**Step 1:** In *subscription* overview page, select “**Budgets**” then “**+ Add**” setup budget and create alerts.

storage\_subscription | Budgets

Subscription

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Security

Events

Cost Management

Cost analysis

Cost alerts

**Budgets**

+ Add

Refresh

Help

Scope : storage\_subscription

We value your feedback! Participate in our

Name Scope

You do not have any budgets.

In the *Create budget* page, fill out the budget details, budget amount information then select “**Next**” to “**Set alerts**”

**Name:** ContosoHC\_Storage\_1  
**Reset period:** Monthly  
**Creation date:** 2023, September 1  
**Expiration date:** 2024, September 30  
**Amount:** 200

## Create budget

Budget

Create a budget and set alerts to help you monitor your costs.

### Budget scoping

The budget you create will be assigned to the selected scope. Use additional filters like resource groups to have your budget monitor with more granularity as needed.

Scope

storage\_subscription

Filters

ResourceType : microsoft.storage/storageaccounts

Add filter

### Budget Details

Give your budget a unique name. Select the time window it analyzes during each evaluation period, its expiration date and the amount.

\* Name  ✓

\* Reset period  ▾

\* Creation date  ▾  ▾  ▾

\* Expiration date  ▾  ▾  ▾

### Budget Amount

Give your budget amount threshold

Amount \*  ✓

Note: I use the filters for a granularity budget scoping for my resources.

**Step 2:** In the *Set alerts* page, select the type of condition “**Actual**”, percent of the budget “**75**” which will display the amount of the budget. For the alert recipients, I will add the “**IT Manager email**” and select “**Create**.”

✓ Create a budget   **2 Set alerts**


Configure alert conditions and send email notifications based on your spend.

**\* Alert conditions**

Type	% of budget	Amount (USD)	Action group
Actual	75	187.50	None
Select type	Enter %	-	None

[Manage action group](#) ⓘ

**\* Alert recipients (email)**

Alert recipients (email)	
nthompson@contosohealthcareUS2023.onmicrosoft.com	
example@email.com	

*It is recommended to add azure-noreply@microsoft.com to your email white list to ensure alert mails do not go to your spam folder.*

**Language preference**

Select your preferred language for receiving the alert email for all recipients provided above. Default is the language associated to your enrollment.

Languages \*   Default

**In conclusion**, this project enabled comprehensive identity and access management for Contoso Healthcare within their Azure environment per cloud security best practices. Critical activities were undertaken including configuration of core Azure AD services for user identity and authentication, implementing least privilege access with Azure RBAC, enforcing organizational standards through centralized policies, and optimizing cost management.